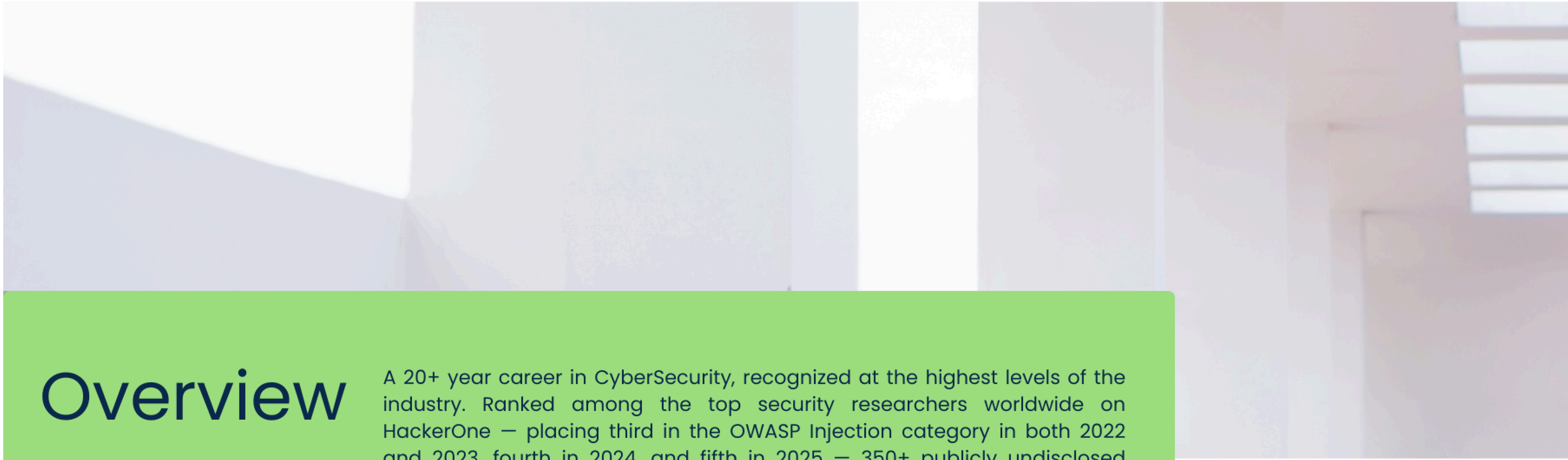
Luca Ercoli - IT Security Specialist

Penetration Testing

Reviewing Achievements and Planning for the Future



Overview

A 20+ year career in CyberSecurity, recognized at the highest levels of the industry. Ranked among the top security researchers worldwide on HackerOne — placing third in the OWASP Injection category in both 2022 and 2023, fourth in 2024, and fifth in 2025 — 350+ publicly undisclosed vulnerabilities have been identified on major platforms including PayPal, eBay, Amazon, Salesforce and the U.S. Department of Defense.

The expertise is backed by industry certifications including Certified Ethical Hacker (CEH), CCNA Routing and Switching, CCNA Security, CCNP Routing — and formally recognized at the highest academic level through a certification approved by Harvard's Office of the Vice Provost for Advances in Learning.

What Is a Penetration Test?

Real-World Attack Simulations

A Penetration Test is a controlled simulation of a cyberattack designed to **identify vulnerabilities** in a company's systems, networks, or applications. Its purpose is to assess the actual level of security, **identify weaknesses before they can be exploited by malicious actors**, and provide concrete recommendations to mitigate them. It is an essential tool for protecting sensitive data, ensuring **business continuity**, and demonstrating compliance with security standards.

How Is a Penetration Test Conducted?

1. **Information Gathering**

In this phase, as much information as possible is gathered about the target, such as IP addresses, domains, subdomains, technologies in use, software dependencies, and public information (OSINT). The goal is to understand the environment and identify potential weaknesses.

2. **Scanning**

The process then moves on to a more technical and automated analysis, using tools for port and active service scanning, vulnerability identification, and operating system and software fingerprinting. The goal is to map the attack surface and identify potential vulnerabilities.

3. **Access**

In this phase, the goal is to exploit the discovered vulnerabilities in order to gain unauthorized access. The most common techniques include exploiting known vulnerabilities, brute-force attacks, SQL injection, XSS, and others. The objective is to gain access to the target system or application.

4. **Maintaining Access**

Here, the attacker’s ability to maintain access is tested, for example by installing backdoors, performing privilege escalation, and establishing persistence within the system. The objective is to simulate an attacker who remains inside the system over an extended period of time.

5. **Analysis and Reporting**

Finally, the results obtained are analyzed and a report is prepared, including the vulnerabilities identified, the techniques used, the compromised data documented, and recommendations for mitigation. The objective is to provide a clear and useful overview for addressing and resolving security issues.

Main Pentesting Approaches

WHITE-BOX

The tester has full visibility into the environment being tested, such as technical documentation or source code.

BLACK-BOX

The tester has no information about the system and behaves like a real external attacker.

GRAY-BOX

The tester has partial access to information, such as the overall architecture and how the APIs work.

The main difference between these approaches lies in the level of knowledge the tester has about the system being assessed.

Realistic External Hacker Test

Realistic External Hacker Test	Black-box
Audit with Source Code Access	White-box
Semi-Internal User Simulation	Gray-box
Project in the Development Phase	White-box

What risks are highlighted by a penetration test?

By way of example and not exhaustively

Insecure Configurations and Technologies

- Services configured in an insecure manner
- Applications affected by publicly known vulnerabilities or vulnerabilities yet to be discovered
- Operating systems running software that can be used as a vector for cyberattacks
- Security settings that are no longer adequate in light of technological advancements

Application-Side Credential and Permission Issues

- Weak, stolen, or leaked authentication credentials exposed on the Deep Web
- Inadequate session management (e.g. predictable IDs or sessions that are not properly invalidated)
- Cookie theft or manipulation (session hijacking/fixation, cookie tampering)
- Access to resources without adequate permission controls

Application Vulnerabilities

- Vulnerabilities that allow an attacker to access your data
- Security weaknesses affecting API services
- The possibility for an attacker to include remote files or execute arbitrary commands on the server hosting your application
- Identifying the attack vectors that enable the injection of malicious code

Protocol- and Architecture-Based Attacks

- Server-Side Request Forgery to force your application to send requests to internal or external systems
- Open Redirect vulnerabilities
- XML External Entity (XXE) attacks
- Inefficient regular expressions that can be exploited for Denial-of-Service attacks

Exposure of Sensitive Services and Resources

- Attempts to gain unauthorized access to sensitive files
- Internal services exposed by mistake (e.g. debug interfaces, admin panels)
- Verification of direct access to restricted objects or files
- Exposure of critical resources or endpoints to unauthenticated users

Can It Be Considered Part of Quality Assurance and Risk Assessment?

PENETRATION TESTING IN THE QUALITY ASSURANCE CYCLE

In the context of QA, the main objective is to ensure that the software functions correctly and meets the requirements. However, security is a fundamental aspect of software quality, so security testing falls within the scope of QA when considering the overall quality of the product.

ASSESSING RISK WITH REAL DATA

Risk assessment is a process aimed at identifying, analyzing, and evaluating security risks affecting a system or an organization. Penetration testing fits into this context as a practical tool for identifying exploitable vulnerabilities and assessing how effectively an attacker could actually compromise the system. It therefore helps validate the assumptions made during the risk assessment and measure the real level of exposure.

The 5 Hidden Costs of a Security Incident

1. FINANCIAL LOSSES

Cybercriminals can access systems and **steal sensitive data** to use for fraud, identity theft, or other illicit purposes. After a breach, companies face significant expenses for **data recovery, forensic analysis, and legal assistance**.

2. BUSINESS INTERRUPTION

An attack can make the website or **systems inaccessible** both internally and to customers, causing financial losses.

3. LOSS OF INTELLECTUAL PROPERTYE

Attacks may target **proprietary software, confidential projects, or strategic plans**. The stolen information may be sold or disclosed, compromising the competitive advantage.

4. REGULATORY VIOLATIONS

Failure to protect personal data can **violate** regulations such as the **GDPR**, resulting in fines and **legal obligations.** Companies may be sued by affected users or partners.

5. REPUTATIONAL DAMAGE

A breach, especially if customer data is involved, undermines trust and can lead customers to **abandon the brand**, damaging the company's image.

Frequently Asked Questions

1.

How much does a Penetration Test cost?

If you are looking for a quick initial check, we can offer a light automated scan starting at approximately EUR 350-500 for very limited scopes, or EUR 800-2,500 for a vulnerability assessment with reporting on small environments.

If, on the other hand, the goal is a manual security assessment with technical validation and more in-depth analysis, the typical budget starts at around EUR 4,000-5,000 and increases depending on scope and complexity.

The quotation is usually calculated by combining several factors: the number of targets to be tested, the type of assets involved (such as web applications or APIs), the complexity of the application flows, the number of user roles, and other similar elements.

2.

How long does it take?

The time required for a penetration test varies depending on the scope and complexity. On average, the technical testing phase can take from 3-5 days for a limited scope to 1-2 weeks or more for more complex environments; when also considering scoping, analysis, and the final report, the entire project may take approximately 2-6 weeks.

3.

Is a staging environment required for a penetration test?

We can work in both production and staging environments. Production is the most useful option when the goal is to measure real-world risk, because it reflects the actual environment an attacker would encounter, including real configurations, integrations, and behaviors.

If staging closely mirrors production, it is usually the preferred choice, also because it can help speed up testing and allow a greater number of requests to be executed in parallel.

When working in production, testing is generally carried out at a request rate designed to avoid degrading the resources of the asset under analysis.

4.

What information do you need to get started?

To begin the engagement, we need to understand which scope you would like us to assess, for example URLs, IP addresses, or APIs.

If the scope includes authenticated areas, you will need to provide valid credentials.

Where different user roles exist, we usually require one account for each relevant role, for example a standard user and an administrator, so that we can properly assess the attack surface and the different authorization levels.

Based on this information, we can quickly provide an estimate of timing and pricing.

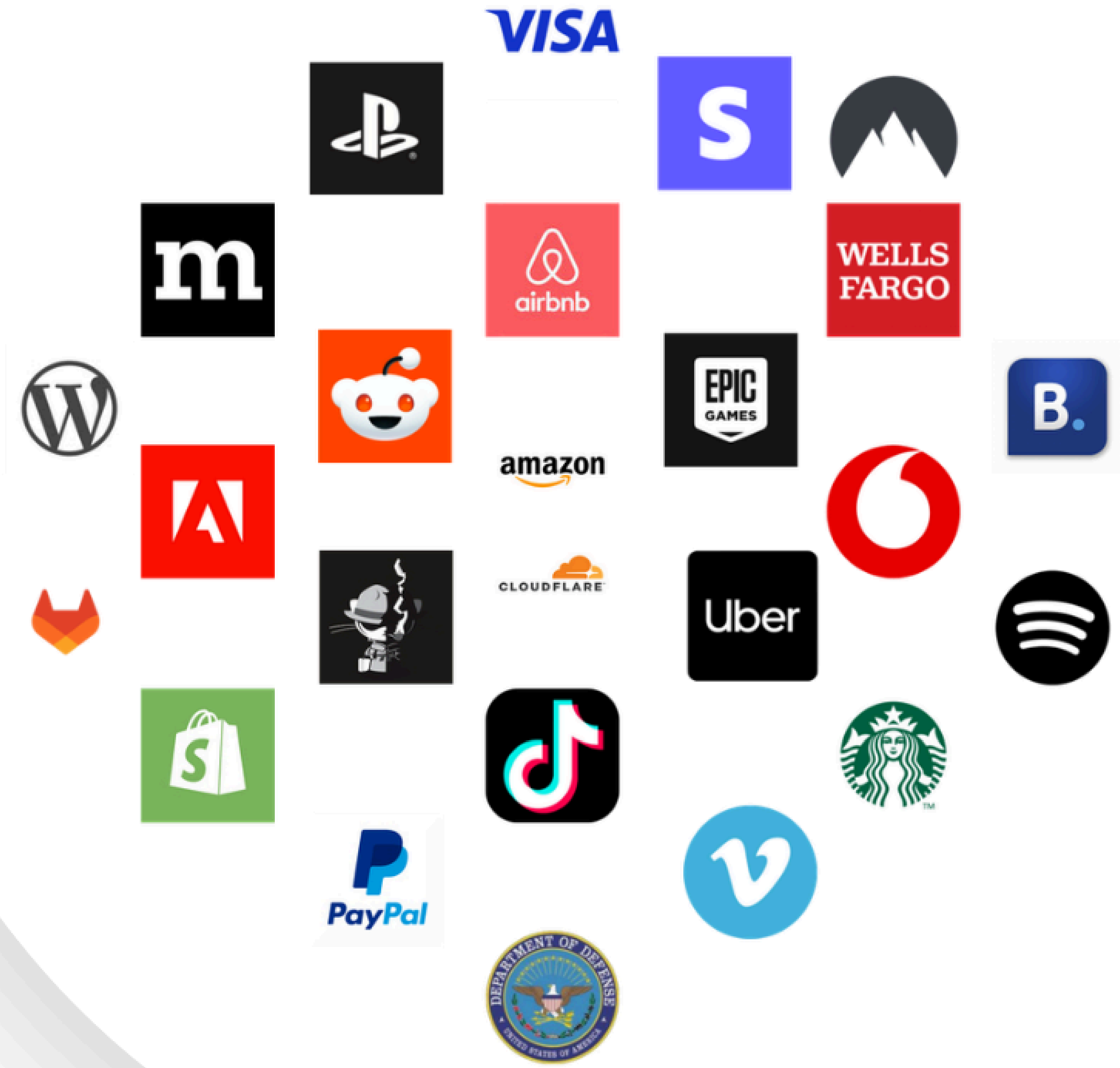
Satisfied Customers

Companies that have used our services

Here are some of the notable companies whose systems I have successfully helped secure through professional penetration testing and vulnerability assessments.

What did the Mozilla Foundation communicate?

> ***When asked about working with krynos on a vulnerability submission, Mozilla said... "Krynos provided us with a well written and detailed report, using a novel attack."***



Protect your sensitive data today and ensure business continuity

Request Your Penetration Test

We are ready to assist you

A controlled simulation of a real-world cyberattack, designed to uncover vulnerabilities in your systems — whether websites, API servers, networks, or applications. The goal is to assess your actual security posture, identify weaknesses before malicious actors can exploit them, and provide actionable recommendations to mitigate risks.

🌐 lucaercoli.it
✉ luca@lucaercoli.it